Secure management of IoT devices lifecycle through identities, trust and distributed ledgers

D6.6 - Plan on Standardization Activities

Document Summary Information

Grant Agreement No	101020416	**Acronym**	ERATOSTHENES
Full Title	Secure management of IoT devices lifecycle through identities, trust and distributed ledgers		
Start Date	01/10/2021	**Duration**	42 months
Project URL	www.eratosthenes-project.eu		
Deliverable	D6.6 - Plan on Standardization Activities		
Work Package	WP6		
Contractual due date	31/08/2023	**Actual submission date**	31/08/2023
Nature	Report.	**Dissemination Level**	Public
Responsible author	UMU	**Lead Beneficiary**	Universidad de Murcia
Authors	Antonio Skarmeta, Agustin Marin, Manel Rodriguez, Michail Bampatsikos, Konstantinos Loupos, Dimitri Van Landuyt, Konstantinos Krilakis		
Internal reviewers	KUL, EUL		

Revision history (including peer reviewing & quality control)

Version	Issue Date	% Complete	Changes	Contributor(s)
v0.1	05/06/2023	20%	First draft version	Antonio Skarmeta, Agustin Marin
v0.2	06/06/2023	30%	Initial sections and content	Antonio Skarmeta, Agustin Marin
v0.3	13/06/2023	50%	First fill of sections	Antonio Skarmeta, Agustin Marin
v0.4	14/06/2023	70%	Filling sections	Antonio Skarmeta, Agustin Marin
v0.5	15/06/2023	80%	Filling structural sections	Antonio Skarmeta, Agustin Marin
v0.8	27/07/2023	90%	Filling section 4	Konstantinos Loupos, Manel Rodriguez, Michail Bampatsikos
v1.0	27/07/2023	100%	Update section 3, conclusions, table of contents, typos, executive summary, etc.	Agustin Marin, Antonio Skarmeta.
v1.1	29/08/2024	100%	Document updated and revised based on reviews.	Agustin Marin, Antonio Skarmeta, Dimitri Van Landuyt, Konstantinos Krilakis

Disclaimer

Copyright message

Table of Contents

Tables

Table of Figures

Glossary of terms and abbreviations used

Abbreviation / Term	Description
3GPP	3rd Generation Partnership Project
AI	Artificial Intelligence
AIOTI	Alliance for the Internet of Things Innovation
ANSI	American National Standards Institute
CEN	European Committee for Standardization
DLT	Distributed Ledger Technology
ECSO	European Cyber Security Organisation
eIDAS	Electronic Identification, Authentication and Trust Services
ESI	Electronic Signature Infrastructure
ETSI	European Telecommunications Standards Institute
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information and Communications Technology
IoT	Internet of Things
ISG	Industry Specification Group
M2M	Machine to Machine
PDF	Portable Document Format
SME	Small and Medium-sized Enterprises
TC	Technical Committees
TPS	Trust Service Providers
WG	Working Group

Executive Summary

This document serves as the main reference for the standardization activities within the ERATOSTHENES project. The standardization plan has been designed through the collaboration of all project work packages to ensure consistency with the overall project objectives. The plan is intended to set the main guidelines for project partners to help identify and take advantage of opportunities to advance the ERATOSTHENES vision and achievements around standardization.

The project work package responsible for standardization activities is fundamental and cross-cutting to all other work packages, underscoring the importance of standardization to the overall success of the project. In line with this, each work package has made a distinctive contribution to the formulation of this deliverable.

The document showcases pivotal contributions to standardization, a testament to the diligent endeavors of our team in tandem with our partners. To provide clarity on our current position in the standardization activities: we've already pinpointed our primary standardization bodies, namely AIOTI, ISO, eECSO, and ETSI. Furthermore, we have obtained specific outcomes related to these standardization bodies from multiple partners, strengthening the project's leadership and building trust and recognition in the field. We are currently progressing through the second of three phases in our standardization activities. Through these actions, we are solidifying our pledge to excellence while nurturing innovation and synergies within the sector.

As we move forward, it's crucial to emphasize that this document signifies the initial endeavors in the realm of standardization for the ERATOSTHENES project (D6.6 - M23). Yet, in the upcoming Deliverable: D6.13 - Report on Standardization Activities, we commit to providing an exhaustive overview of our advancements and milestones in standardization in an in-depth manner.

1 Introduction

The standardization activities aim to foster widespread adoption, integration, and interoperability across various sectors. These activities focus primarily on three critical realms: automotive, health, and Industry 4.0; application areas related to the pilots proposed and currently in development in ERATOSTHENES. The end goal is to develop validated and benchmarked solutions that address real-life scenarios in these sectors, supported by rigorous standardization approaches.

- In the automotive sector, standardization efforts play a crucial role in addressing the increasing complexity of vehicle systems, with a specific focus on areas such as autonomous driving, vehicle-to-vehicle (V2V) communication and communication vehicle to Things (V2X). By actively promoting standardization, we aim to facilitate the seamless integration of these technologies, minimize the likelihood of conflicts between systems and further improve safety and efficiency.

- In the healthcare sector, standardisation activities focus on the creation of validated and reference solutions to improve patient care, increase diagnostic accuracy, and foster interoperability between different healthcare systems.

- In the context of Industry 4.0, standardisation activities aim to support the seamless integration of digital technologies into industrial processes. They focus on the development of standardised protocols for machine-to-machine communication, data security and the application of advanced technologies such as AI and IoT.

1.1 Mapping ERATOSTHENES Outputs

Purpose of this section is to map ERATOSTHENES Grant Agreement commitments, both within the formal Deliverable and Task description, against the project's respective outputs and work performed.

Table 1: Adherence to ERATOSTHENES GA Deliverable & Tasks Descriptions

ERATOSTHENES GA Component Title	ERATOSTHENES GA Component Outline	Respective Document Chapter(s)	Justification
DELIVERABLE			
D6.6 - Plan on Standardization Activities	Plan of Standardization activities and developed material including recommendations towards standardization bodies (related to T6.6).	2,3,4	Chapter 2 describes standardization plan. Chapter 3 standardization bodies. Chapter 4 describes standardization activities.
TASKS			
Task 6.6	This task frames all standardisation activities. The project plans to contribute to standardisation via the project partner's	2,3,4	Chapter 2 describes standardization plan.

	membership in standardisation organisations deriving advancements in the area to standards, regulations and activities within reference normative organisations. This task will be also following and promoting the projects results in related communities and initiatives and contribute to the definition of security roadmap on IoT. Define and implement a coordinated set of actions to identify results that are suitable for standardisation into the most relevant standard making bodies. For each of the selected bodies/forums, a partner will be appointed to take the responsibility of the collaboration, advising and supporting on the possible standardisation actions on behalf of the consortium; prepare informational material to influence standardisation via the involved bodies of the partner organisations; make a plan for assuring high-impact of the ERATOSTHENES; create general awareness about project objectives and results; and compile a list of high impact related initiatives and use target audiences, including sectorial associations, initiatives or ecosystems, open source communities, potential "multipliers" (early adopters of technology) and EU Security fora. ERATOSTHENES will contribute to clustering activities promote by the commission and in fora like ECSO to influence future strategic agendas and create collaboration with the European Competence Network of Cybersecurity Centres of Excellence (D6.6, 6.13).		Chapter 3 standardization bodies. Chapter 4 describes standardization activities.

1.2 Deliverable Overview and Report Structure

The following is a description of the Deliverable structure, providing an overview of the different sections and their content.

- Section 1, Introduction of the document.
- Section 2 discusses the aim to standardize technologies and components for better interoperability, scalability, security, consistency, cost-efficiency, and competition in IoT scenarios, with partners committed to contributing to standardization activities and regulatory body monitoring.
- Section 3 discusses different standardization bodies the project will focus for its assets for standards to follow and contributions to do.
- Section 4 outlines the actions and activities that the project and its collaborators plan to undertake during the upcoming phase.
- Section 5, conclusion of the whole document.

2 Standardization plan

The standardization plan in the ERATOSTHENES project aims at standardizing technologies and components to be developed within the project. This approach is of particular significance in IoT scenarios for several reasons:

- Interoperability: Ensuring seamless communication and data exchange between different IoT devices and software from multiple vendors.
- Scalability: Simplifying integration of new devices.
- Security: This is vital in an IoT context where significant volumes of potentially sensitive data are transferred. Everyone following the same set of guidelines makes it easier to detect potential vulnerabilities.
- Consistency: Standardization assists in managing the inherent complexity of an environment populated with thousands of interacting devices utilizing various programming languages and technologies. It ensures that data collected from these diverse devices is consistent and comparable.
- Cost-efficiency: Through standardization, the cost-efficiency of both production and management of devices can be improved by reducing time, cost of development and learning curve.
- Innovation and Competition: Standardization paves the way for innovation by providing a stable platform for companies to compete, leading to more efficient, effective, and creative solutions.

Our partners will dedicate themselves to contributing to standardization activities, with a focus on maximizing the impact of the outcomes. This will involve monitoring regulatory bodies and open-source projects. Our partners are committed to thoroughly exploring and participating in opportunities to contribute to technical specifications, working groups, software elements, proofs of concept, and white papers.

In order to structure and optimise our efforts in the field of standardisation, we have defined a series of phases that outline our process:

- Phase 1 (Completed): Early identification of potential standardisation bodies and their respective Working Groups Technical Committees for future contributions.
- Phase 2 (Ongoing): Final definition and update of target standardisation bodies, together with the first round of contributions.
- Phase 3 (Upcoming): Assessment of the outcomes from our extensive inputs to the standardisation processes and disseminating these findings to pertinent groups and initiatives.

3 Targeted standardization bodies and standards-related organizations

In the diverse landscape of standardization, a multitude of bodies and organizations exist. As our project evolves, we are specifically targeting certain key entities. This section delves into the targeted standardization bodies and other pertinent standards-related organizations currently in focus.

3.1 AIOTI

AIOTI, or the Alliance for the Internet of Things Innovation, is an organization that leads a dynamic European IoT and Edge Computing ecosystem.

Established in 2015, AIOTI works on behalf of their members to drive business, policy, standardization, research, and innovation development in the IoT and Edge Computing. Focuses on other converging technologies, across the Digital Value Chain to support European digitization and competitiveness. Involves in various activities, including promoting the convergence of Edge Computing standards within the international community and identifying gaps related to semantic interoperability standards and technologies within and across IoT domains, including smart living environments for ageing well, smart farming and food security, wearables, smart cities, and many more. As a key player in the IoT landscape, works towards a connected and innovative future where IoT technologies are leveraged to their full potential[1].

This organization operates in various collaborative groups, including working groups, focus groups, and task forces. These working groups are also divided into[2]:

- Horizontal Working Groups: areas applied to any sector.
    - Policy, Research and Innovation, Standardization, Testbeds.
- Vertical Working Groups: domain-specific areas.
    - Agriculture, Energy, Health, Manufacturing, Mobility.
- Task Force: specific topics inside a working group.
    - Digital for climate, Early Innovation Champions, Web3 Accelerator.

The aim of the project is to utilize the collaboration of multiple partners within the consortium. These partners are actively involved in the working group called WG03[3], which is dedicated to standardization activities, and it is described in section 4.1.

3.2 ISO

The International Organization for Standardization (ISO) serves as a pivotal force in the development of globally recognized standards, fostering collaboration and unity among nations. Comprising standards bodies from over 160 countries, ISO's diverse membership is represented by a single standards body per member country, such as the American National Standards Institute (ANSI) for the United States. By establishing shared standards, ISO aims to enhance efficiency, safety, and compatibility across industries worldwide. Compliance with ISO standards not only provides companies with a competitive advantage but also increases consumer confidence and promotes sustainable development practices. With its consensus-driven approach and inclusive membership, ISO continues to shape the future of global standardization[4].

Within ISO, Technical Committees (TCs) are instrumental in standardizing various fields. These committees span a wide spectrum, ranging from TC1, established in 1947 and focused on screw threads, to more recent TCs like TC 323, dedicated to standardizing the circular economy. Each TC is headed by a chairman, while an ISO member holds the

[1] https://aioti.eu/
[2] https://aioti.eu/groups/
[3] https://aioti.eu/about-us/our-groups/standardisation/
[4] https://www.iso.org/about-us.html

secretariat role, ensuring effective coordination and administrative support. The program of work for each TC provides insight into upcoming meetings and the ongoing development of standards in the pipeline[5].

Working Groups (WGs) are set up as part of the preparatory stage for a new standard. They are composed of subject matter experts and industry stakeholders. Once the WG prepares a working draft of the new standard that is deemed satisfactory, the WG's parent committee (usually a TC) decides which stage occurs next.

To address cybersecurity incidents and minimize their consequences, ERATOSTHENES and its partners propose the adoption of a solution built upon distributed trust and digital identity management. This solution aligns with the standards set by ISO/TC 22/SC 32/WG 11; a joint working group established under ISO. Breaking down the topics that each of the mentioned groups is focusing on: TC 22: Road vehicles; SC 32: Electrical and electronic components and general system aspects and WG 11: Cybersecurity[6]. In summary, ERATOSTHENES focuses on cybersecurity, specifically in electronic components related to road vehicles, detailed in section 4.2.

3.3 ECSO

Established in 2016, the European Cybersecurity Organization (ECSO) serves as the primary independent entity across all sectors for cybersecurity in Europe, engaging public and private stakeholders in cooperative efforts. It functions as a platform for collaboration between diverse entities including large corporations, small to medium enterprises, start-ups, academic institutions, essential service operators, associations, and local to national public administrations from EU Member States, EFTA, and H20201 associated countries. ECSO's principal objective is to enhance Europe's digital sovereignty, strategic autonomy, and cyber resilience by fostering a robust cybersecurity ecosystem and promoting effective dialogue and actions between the private and public sectors[7].

ECSO standardization flow works through six working groups[8]:

- Standardization, certification, and supply chain management (WG 1): Focuses on the establishment of trusted and resilient supply chains in Europe by supporting the rollout of EU ICT security certification schemes and understanding the industry's challenges1.
- Market deployment, investments, and international collaboration (WG 2): Aims to boost private investments in the European cybersecurity industry and promote Europe-based cybersecurity products overseas, while also improving market knowledge among ECSO members.
- Cyber resilience of economy, infrastructures, and services (WG 3) under ECSO aims to create a trusted environment for cybersecurity practitioners and end-users to share information, learn from experiences, and develop best practices to enhance the cyber resilience of European companies and organizations.
- The Support to SMEs, coordination with countries and regions (WG 4) initiative fosters a strong European community of cybersecurity SMEs, promotes cooperation among regions, and enhances the competitiveness of local startups at the European level.
- The Education, Training, Awareness & Cyber Ranges (WG 5) under ECSO aims to foster an ecosystem of cybersecurity education and training to support and influence all European cybersecurity stakeholders.
- The SRIA and Cybersecurity Technologies (WG 6) aims to analyze the European cybersecurity ecosystem, identify gaps and opportunities, and promote innovative solutions of the European SMEs to accelerate the digital sovereignty of Europe.

Open international standards play a crucial role in stimulating market development across various business sectors. They foster sustainability and interoperability, creating a competitive environment for equipment, service, and content providers. In this context, the project intends to leverage the expertise of working groups, involving project partners, to contribute to critical standards. For instance, the working group ECSO – WG1[9] will provide recommendations for cybersecurity standards, certification, and labeling. In section 4.3, there is a comprehensive explanation of the reasons behind our decision to prioritize the ECSO - WG1 group.

[5] https://www.iso.org/committee/6266604.html
[6] https://www.iso.org/committee/5383636.html
[7] https://ecs-org.eu/who-we-are/
[8] https://ecs-org.eu/activities/
[9] https://ecs-org.eu/activities/standardisation-certification-and-supply-chain-management/

3.4 ETSI

ETSI, the European Telecommunications Standards Institute, is a renowned body that places a significant emphasis on identity, security, digital identity, and distributed trust management in the realm of information and communications technology (ICT), among a multitude of factors. Offering an open, inclusive, and collaborative platform, it facilitates the prompt development, endorsement, and verification of universally-applicable standards for ICT-driven systems, applications, and services.

Leading the way in emerging technologies that utilize ICT across all industry sectors and societal dimensions, ETSI's network extends across more than 60 countries and five continents, uniting over 900 member organizations. As a non-profit entity, it is one of the few institutions officially acknowledged by the EU as a European Standards Organization.

While ETSI's origins lie in catering to European needs, it now pursues a global perspective, with its standards being implemented worldwide. It operates synergistically with various global organizations, enabling it to effectively support its members in an increasingly international and competitive landscape. ETSI also actively collaborates on a global scale in projects such as oneM2M to establish standards for machine-to-machine communications, placing an emphasis on secure digital identity and trust management[10].

From ETSI technical groups, we identify these categories[11]:

- ETSI Partnership Projects: established when there is a need to cooperate with other organizations to achieve a standardization goal (3GPP and oneM2M)
- Committees, projects, and other groups: Technical Committees (TCs) focus on specific technology areas for standardization; ETSI Projects (EPs) address market-specific needs; Software Development Groups (SDGs) combine standardization with software development; Special Committees (SCs) handle coordination and requirement gathering; Specialist Task Forces (STFs) consist of experts performing specific technical tasks.
- Industry Specification Groups: these operate alongside our traditional standards-making committees in a specific technology area. They are designed to be quick and easy to set up. They provide an effective alternative to the creation of industry fora.

For ERATOSTHENES, there are multiple working groups in ETSI that provide a space to showcase emerging technologies and validate them against new regulations, in addition to allowing participation in the results of initiatives focused on the creation of standards that enhance the security and privacy of entities and individual subjects. However, project partners will focus especially on ETSI CYBER TC which targets on cyber security for home gateways and specifically in the realm of the consumer Internet of Things. Its primary objective is to establish a comprehensive framework for evaluating the adherence to essential security requirements. The project will also center its attention on the TC ESI (Electronic Signature Infrastructure) which encompasses digital signatures, procedures, and policies for their creation and validation. It covers security requirements for trust service providers and aims to support the eIDAS Regulation and confidence in electronic transactions, including trusted lists for approved TSPs[12]. Finally, not only will we direct our attention to the TCs, but also to ISGs such as: ISG ITS and ISG SAI.

The ERATOSTHENES project and its partners prioritize end-to-end communication, distributed trust management, and digital identity to achieve a high impact and significant reduction in several cybersecurity incidents within the IoT domain. This is further detailed in section 4.4.

[10] https://www.etsi.org/about

[11] https://www.etsi.org/about/our-operations

[12] https://www.etsi.org/committees

4 Standards-related activities

Efforts will be concentrated on providing support to the technical and development workgroups operating within the scope of ERATOSTHENES. This support will span various areas, including logistics, advice, and recommendations, all aimed at identifying the appropriate standardization bodies for each asset within the project and promoting contributions to standardization. The progress of each standardization activity will be monitored, with each effort diligently undertaken by the designated work package.

There will be a collaborative exchange of information between the work packages and partnerships. We plan to share knowledge from standardization bodies and associated organizations such as open-source entities. This will facilitate adherence to and contribution towards established guidelines.

In the previous section we introduced the standardization bodies, with a brief description of their structure and functioning when it comes to approval processes. As the project is in its technical and development phase and our partners are carefully developing the assets, following best practices to ensure quality contributions to standardization, courtesy of the project partners' membership in standardization bodies. Although the following contributions may seem modest, these actions lay a solid foundation that will transcend the duration of the project, encouraging future activities with valuable results.

4.1 Contribution in AIOTI Standardization WG

ERATOSTHENES intends to take advantage of the participation of several consortium partners in the AIOTI (Alliance of Internet of Things Innovation) such as INLE and UMU. These partners are strongly engaged in the relevant working group (WG03) that is dedicated to standardization activities.

The AIOTI WG03 (Standardization) overall vision is to "*be recognized as a major contributor to the worldwide interoperability, security, privacy and safety of IoT systems and applications, and particularly for the development of the market in EU*".

On top, ERATOSTHENES fully supports the overall vision of WG03 defined as "*The work of AIOTI WG03 is seen as a reference for the AIOTI Working Groups in order to address the interoperability issues and to recommend the use of standard-based solutions for the deployment of IoT solutions. We have been talking to SDOs and Alliances about collaborations and interworking as a means to reduce fragmentation. What AOITI brings to all is a dramatic acceleration of the pace of those discussions*" [1].

The priorities of this WG can be summarized to:

- Maintaining an IoT & Edge Computing standards framework landscape
- Conducting gap analysis
- Defining the Computing Continuum
- Designing High-Level Architectures for IoT, Edge Computing, and Digital Twins
- Evaluating IoT relation and impact on 5G and Beyond 5G
- Ensuring Semantic Interoperability
- Enhancing security and privacy in the computing continuum
- Establishing and maintaining collaborations

The activities of interest of ERATOSTHENES are fully aligned with the project scope and include the following prioritized activities:

- High Level Architecture for IoT, Edge Computing and Digital Twins
- IoT & Edge Computing standards framework landscape
- Security and Privacy

Regarding security and privacy activities that are considered to be of primal interest and priorities for ERATOSTHENES, we include below the particular focus of interest and intended contribution (in bold) [2]:

Privacy:

- **GDPR conformance of communications and data storage in an IoT network and in devices**
- Careful identification of properties of devices, restriction to absolutely necessary data details, etc.
- **Anonymity preservation: considering their different roles in various applications, including AI aspects, transparency in processing, disclosure/transfer control, threat analysis, certification, encryption, best practices for compliance, stakeholder roles/rights/responsibilities, domains: personal tracking (from fitness apps to electronic tickets for public transport, healthcare, smart home), de-personalization of data to safeguard privacy (e.g. when building digital twins)**
- **Assessment and certification/qualification: threat analysis, certification, best practices for compliance, stakeholder roles/rights/responsibilities for IoT/Edge Computing (e.g. devices, infrastructures, platforms)**
- **Privacy in complex systems/system of systems (e.g. edge analytic, data spaces, digital twins, AI systems), network, service, resource and data orchestration and decentralization**

Security:

- **Cybersecurity assurance of complex system (digital twins, AI systems)**
- **AI based threat detection and classification.**
- Security of edge processing
- IoT/Edge computing related to human & infrastructure safety and security in various applications including AI aspects.
- Security and privacy of autonomous vehicles and drones
- Physical security of unattended devices; cybersecurity, security and privacy of verticals (e.g. health, manufacturing, mobility and critical infrastructure)

The vertical industrial domains of AIOTI WG03 have also been considered and seem aligned to the overall approach of ERATOSTHENES and its wide requirements as a refence architecture, as shown below:

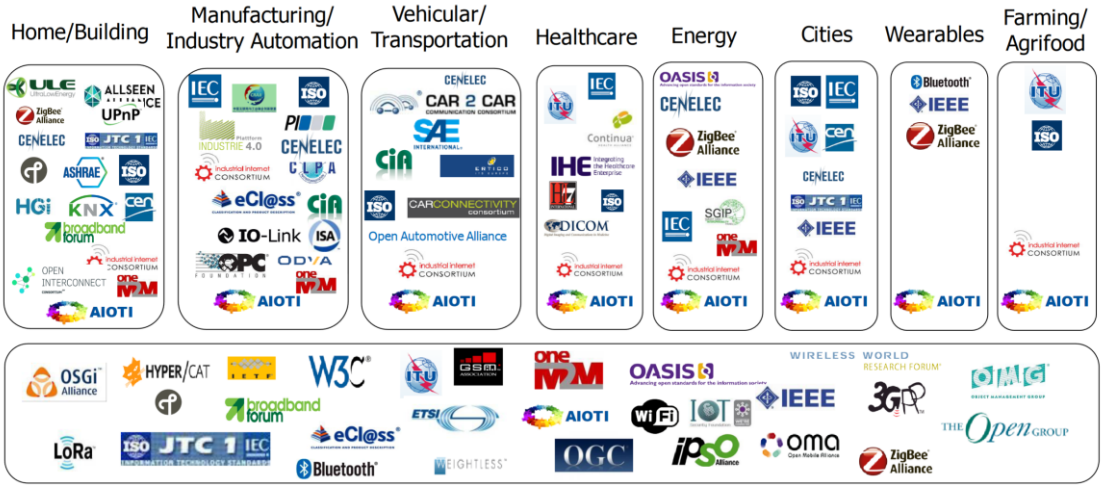

Figure 1 AIOTI WG03 vertical and horizontal activities

AIOTI is contributing in particular to the ETSI standardization body through a list of documents consolidated as recommendations towards the several body priorities. The means are summarized below, and indicative documents of the last months are listed as examples in which the ERATOSTHENES consortium intends to strongly contribute.

- AIOTI High Priority IoT Standardization Gaps and Relevant SDOs Release 2.0 - AIOTI WG03 [3]
- AIOTI IoT and Edge Computing EU funded projects landscape Report [4]
- AIOTI High Level Architecture (HLA), Release 4.0, AIOTI WG03 – IoT Standardization [5]
- AIOTI Report High Priority Edge Computing Standardization Gaps and Relevant SDOs [6]
- AIOTI Identifiers in Internet of Things (IoT) Release 1.0 [7]

The identified contribution of this WG towards some of the ISO/IEC includes the following that will be also investigated during the course of the task execution:

- ISO/IEC27115 – Cybersecurity evaluation of complex systems
- ISO/IEC 27091 – AI privacy protection
- ISO/IEC 27568 – Security and privacy of digital twins

Other possible examples of contributions include:

- Contribution to the public consultation on EU Standardisation Strategy Roadmap [8]

To conclude on the ERATOSTHENES involvement in standards through the AIOTI, ERATOSTHENES intends to keep its high involvement in this and other WGs (IoT, research and innovation etc.). The consortium will contribute to related activities, similar to the above, that will be running in the next years and until the end of the project. The intention is to provide valuable inputs coming from the ERATOSTHENES research level but also its real industrial deployments, towards to bodies that can pave the way towards standardization (at any level). In this, we consider AIOTI of primal importance and a contributor of high impact. At the same time, the ERATOSTHENES contribution is not considered to be 'stand alone' or on its own. Liaison with other projects, outside and inside AIOTI, will strongly support our scope and intentions in creating valuable but also realistic contributions over standards.

4.2 Contribution in ISO/TC 22/SC 32/WG 11 "Cybersecurity"

Within the global realm of information and cybersecurity, international standards play an indispensable role in fortifying systems, establishing trust, and facilitating commerce. Recognizing the criticality of such standards, particularly in the fast-evolving automotive sector, ISO/TC 22/SC 32/WG 11 titled "Cybersecurity" has been at the forefront of these efforts.

WG objectives:

- Develop international standards to help organizations protect their information systems against security threats.
- Promote the use of international information security standards around the world.
- Facilitate international trade by ensuring that organizations around the world comply with the same information security standards.
- Help organizations reduce the costs associated with information security.
- Improve information security overall.

The working group is composed of representatives from organizations around the world, including governments, businesses, and standardization organizations. The group meets regularly to discuss the latest developments in information security and to develop international standards.

The WG has developed the referent ISO in automotive cybersecurity; ISO 21434 is based on the software development lifecycle and provides a framework for cybersecurity risk management, threat identification and assessment, implementation of security controls, security testing, and operation and maintenance of security systems. The standard also covers topics such as security configuration management, information security management, and security training.

There is also the ISO 8475 which is a Publicly Available Specification (PAS) that is currently under development by the ISO/TC 22/SC 32/WG 11 working group. The PAS is designed to provide guidance on the implementation of Cybersecurity Assurance Levels (CALs) and Targeted Attack Feasibility (TAF) in road vehicles.

IDIADA is participating in this working group through the Spanish national committee and can contribute from an Automotive point of view regarding the ERATOSTHENES outputs in case these are relevant for the standards being developed during the working group activities.

4.3 Contribution in ECSO WG1

ECSO WG1 - Standardisation, Certification and Supply Chain Management, part of the European Cyber Security Organization, plays a crucial role in enhancing Europe's cyber resilience. It emphasizes standardization, certification, and supply chain management to ensure a cohesive and secure ICT approach across the EU, especially vital given the rapid growth of the digital world.

1. The objective of this WG is to support the roll-out of EU ICT security certification schemes, standard and legislative recommendations, and ensure the establishment of trusted and resilient supply chains in Europe.
2. Current works:
    1. Composition approach across EU schemes
    2. Guidelines for the certification of secure systems and analysis of the associated risk management.
    3. Identify the challenges for SMEs in using certification schemes and define guidelines / best practices (survey)
    4. Address the challenges for a trusted supply chain and management of the risks.
    5. Analysis for consistency of the legislative framework and Cybersecurity Act and potential market impact.
    6. Analysis of the Cyber Resilience Act proposal
    7. Collaboration with ENISA, EC, European SDOs and other relevant stakeholder with feedback

The current UMU contribution has been:

- Composition approach across EU schemes. Challenges on how to reuse certification information from the same and from different schemes.
- KPIs and Metrics of Certification Schemes to measure their effectiveness and efficiency. Survey to provide feedback to ENISA on the suitability of the metrics.
- Union Rolling Work Program (URWP). Survey to provide feedback to ENISA (areas of future reflection, standardization activities to be prioritized, the IoT dimension…)
- Taxonomy to classify IoT devices (roundtable to collect feedback)
- ECSO's Task Force on Cloud Security Data Spaces (CSDS) – In progress
- Position Paper on the European Cybersecurity Certification Scheme for Cloud Services (EUCS) and Certification composition

4.4 Contribution in ETSI TCs and ISGs

UPRC is a member of ETSI and has requested to participate in the Technical Committee CYBER, which is the most cyber security-oriented Technical Committee, and in the Electronic Signatures and Infrastructures. Both of these Technical Committees are dedicated to standardisation.

The CYBER Technical Committee (TC CYBER henceforth) is a major trusted center of expertise that:

- Provides advice and guidance to users, manufacturers, network, infrastructure as well as service operators and regulators.
- Collaborates closely with stakeholders in the development of standards that increase privacy and security for organizations and citizens across Europe and worldwide.
- Provides standards that are applicable across different domains such as security of infrastructures, devices, services, and protocols.
- Provides standards with regards to the creation of security tools and techniques.

The Electronic Signatures and Infrastructure (ESI) Technical Committee (TC) coordinates ETSI's activities on digital signatures and focuses on: Digital signatures (signature format, certificates) creation and verification based on the following standards: CAdES (CMS digital signatures), PAdES (PDF digital Signatures) ASiC (Associated Signature Container), and JAdES (Json web signatures): currently under development. Moreover, ESI also focuses on:

- Defining technical profiles and policy requirements for trust service providers for a range of services including: Services supporting signature (e.g., certification authorities, Timestamping authorities), Remote Signature creation and validation functions, registered e-delivery, Registered Emails Information preservation.
- Recommending cryptographic suites for digital signatures.

Besides its participation in TC CYBER and ESI, UPRC will investigate possible contribution to the effort of Industry Specification Groups (ISGs) and Technical Committees (TCs). The work of these TCs [9] and ISGs [10] can be fitted in the following fields:

- Securing technologies and systems
    - Intelligent Transport Systems (ISG ITS): focuses on the development and implementation of Intelligent Transport Systems service provision across the network, for transport networks, vehicles and transport users, including interface aspects, multiple modes of transport and interoperability between systems.
    - Securing Artificial Intelligence (ISG SAI): Focuses on using AI to enhance security, mitigating attacks that leverage AI, and securing AIs from attacks.
- Security tools and techniques
    - Secure Element Technologies (TC SET): focuses on the development and maintenance of specifications for the Secure Element and its interface to the outside world for use in telecommunication systems, for general telecommunication purposes as well as for Machine-to-Machine (M2M)/IoT communications. The work of this TC comprises the interface, procedures and protocol specifications between the SE and entities used in its managements. Moreover, it encompasses interfaces procedures and protocol specifications used between such entities for the secure provisioning and operation of services making use of the SE.

The outputs of ERATOSTHENES project could contribute to the standardization efforts of the aforementioned TCs and ISGs as follows.

- Intelligent Transportation Systems: The results of the ERATOSTHENES Connected vehicles pilot and in particular *Use Case 1*: *Vehicle-to-Infrastructure and Vehicle-to-Vehicle communication* can contribute to the standardization of the ITS ISG.
- Electronic Signatures and Infrastructure: The results of the tasks related to the ERATOSTHENES Identity Management Module, IoT device certificates, User (Owner, Introducer, Manufacturer) Certificates solutions can contribute to the work of this TC.
- Securing Artificial Intelligence: The results of the ERATOSTHENES Intrusion Detection/Prevention System implementation that will utilize Machine Learning can be of benefit to the efforts of this ISG. That is because part of this ISG's work relates to using Artificial Intelligence to enhance security.
- Secure Element Technologies: The results of some of the ERATOSTHENES pilots' use cases could contribute to the standards of this Technical Committee. Specifically:
    - Pilot 1 – Connected Vehicles: *Use Case 1 – Vehicle-to-Infrastructure and Vehicle-to-Vehicle Communications.*
    - Pilot 1 – Connected Vehicles: *Use Case 2 – Remote software updates*
    - Pilot 3 – Disposable IDs in Industry 4.0: *Use Case 4- Open Source and 3rd party integration* and *Use Case 5- Scalability testing*

CYBER: The results of the ERATOSTHENES project can contribute to the standardization efforts of TC CYBER in a variety of cyber-security areas related to the IoT paradigm. These areas are Intrusion Detection Systems, Physically Unclonable Functions-based Authentication, Threat Modeling and Risk Assessment, Cyber Threat Intelligence sharing, DLT and Smart Contracts-based Trust Management, Self-Sovereign Identity-based Identity Management, Trusted Execution Environments, Trust Evaluation Algorithms, IoT Device's Network Enrolment and Bootstrapping, DLT-based Cyber Threat Intelligence Sharing, and Manufacturer Usage Description-based Access Control lists.

5 Conclusions

The deliverable has presented the standardization plan, current and ongoing standardization activities and outlined and pinpointed different standardization bodies which are the objectives to consider for ERATOSTHENES project and partners.

ERATOSTHENES team will track the approach defined in this document. From the time this document is generated and disseminated, we will oversee and manage activities, expecting outcomes comparable to those shown in this document throughout the project's lifespan.

Additionally, this document has already demonstrated several contributions from various partners, both standardization bodies and related organizations.

Lastly, as we turn our focus towards the upcoming document, we anticipate seeing the fruits of collaboration in the form of publication results from our partners. These partners are associated with some of the entities discussed in this document. We are keen to observe the culmination of their work and efforts, and how these results will contribute to the overall progress and development of our shared objectives.

6 References

[1] AIOTI - ALLIANCE FOR INTERNET OF THINGS INNOVATION, 21-22 March 2016 – IoT in the Smart Home, WG03 IoT Standardisation introduction.

[2] Role of AIOTI WG03 in IoT Standardisation - https://aioti.eu/role-of-aioti-wg03-in-iot-standardisation/

[3] High Priority IoT Standardisation Gaps and Relevant SDOs Release 2.0 - AIOTI WG03

[4] IoT and Edge Computing EU funded projects landscape Report

[5] https://aioti.eu/wp-content/uploads/2018/06/AIOTI-HLA-R4.0.7.1-Final.pdf

[6] AIOTI Report High Priority Edge Computing Standardisation Gaps and Relevant SDOs, April 2022

[7] Identifiers in Internet of Things (IoT) Release 1.0 February 2018

[8] Contribution to the public consultation on EU Standardisation Strategy Roadmap